Amendments to the Claims:

This listing of claims will replace all prior version, and listings, of claims in the application:

Listing of Claims:

1.(currently amended): A method for providing a cryptographic service utilizing a server on a network, comprising:

(a) identifying a client utilizing the network;

(b) establishing a first key;

(c) generating a tunnel on the network;

(d) receiving information at the server from the client utilizing the tunnel, wherein the information is encrypted by the client using the first key; and

(e) performing the cryptographic service at the server for the client whereby the server off-loads a computational burden associated with the cryptographic service from the client.

2.(original): A method as recited in claim 1, wherein a second key is encrypted by the client using the first key, and further comprising receiving the second key at the server.

3.(previously presented): A method as recited in claim 2, wherein the second key comprises at least one parameter for the cryptographic service performed by the server.

4.(canceled)

5.(previously presented): A method as recited in claim 1, wherein the cryptographic service includes modular exponentiation.

6.(previously presented): A method as recited in claim 1, further comprising the step of transmitting cryptographic service results to the client.

7.(previously presented): A method as recited in claim 6, further comprising: the step of encrypting the cryptographic service results utilizing the first key.

8.(previously presented): A method as recited in claim 6, wherein the cryptographic service results are transmitted to a third party.

9.(previously presented): A method as recited in claim 1, further comprising the step of charging a fee for the cryptographic service performed by the server.

10.(original): A method as recited in claim 9, wherein the fee is charged to the client.

11.(original): A method as recited in claim 1, wherein the first key comprises an encryption key for a symmetric cipher.

12.(original): A method as recited in claim 1, wherein the first key comprises an encryption key for an asymmetric cipher.

13.(currently amended): A computer program embodied on a computer readable medium for providing a cryptographic service utilizing a server on a network, comprising:

(a) a code segment for identifying a client utilizing the network;

(b) a code segment for establishing a first key;

(c) a code segment for generating a tunnel on the network;

(d) a code segment for receiving information at the server from the client utilizing the tunnel, wherein the information is encrypted by the client using the first key; and

(e) a code segment for performing the cryptographic service at the server for the client whereby the server off-loads a computational burden associated with the cryptographic service from the client.

14.(original): A computer program as recited in claim 13, wherein a second key is encrypted by the client using the first key, and further comprising a code segment for receiving the second key at the server.

15.(previously presented): A computer program as recited in claim 14, wherein the second key comprises at least one parameter for the cryptographic service performed by the server.

16.(canceled):

17.(previously presented): A computer program as recited in claim 13, wherein the cryptographic service includes modular exponentiation.

18.(previously presented): A computer program as recited in claim 13, further comprising a code segment that transmits the cryptographic service results to the client.

19.(previously presented): A computer program as recited in claim 18, further comprising a code segment that encrypts the cryptographic service results utilizing the first key.

20.(currently amended): A system for providing a cryptographic service utilizing a server on a network, comprising:

(a) logic for identifying a client utilizing the network;

(b) logic for establishing a first key;

(c) logic for generating a tunnel on the network;

(d) logic for receiving information at the server from the client utilizing the tunnel, wherein the information is encrypted by the client using the first key; and

(e) logic for performing the cryptographic service at the server for the client whereby the server off-loads a computational burden associated with the cryptographic service from the client.

21.(previously presented): A method as recited in claim 3, wherein a message or a cyphertext comprises a second parameter for the cryptographic service performed by the server.

22.(original): A method as recited in claim 21, wherein the message or cyphertext has been blinded by the user before transmittal to the server.